UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA
JOHNSTOWN DIVISION

In re Conemaugh Pixel Litigation	Case No. 3:23-cv-00110-SLH **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs TACEY HABERKORN and JANE DOE, individually, and on behalf of all others similarly situated, (hereinafter "Plaintiff") bring this Class Action Complaint against Defendants, DUKE LIFEPOINT HEALTHCARE, LLC; DLP HEALTHCARE, LLC; DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC; DLP PHYSICIAN PRACTICES, LLC; DLP CONEMAUGH JV, LLC; DLP CONEMAUGH HOLDING COMPANY, LLC; and JOHN DOES 1-5 (hereinafter "Conemaugh" or "Defendants"), and alleges, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiffs bring this class action to address Defendants' improper practice of disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiffs and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] Google, LLC ("Google"), DoubleClick, Kenshoo, CallRail, and potentially others ("the Disclosure"), via tracking technologies used on its website.

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendants', that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on Defendants' website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Conemaugh is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiffs' reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

[4] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[5] *Id.*

including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[6]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.[7] If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. The need for data security (and transparency) is particularly acute when it comes to the rapidly expanding world of digital healthcare as, of all the information the average internet user shares online, health data is some of the most valuable and controversial.[8]

---

[6] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

[7] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk*, WIRED (Nov.16, 2022) https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited May 1, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022) https://themarkup.org/pixel- hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited May 8, 2023).

[8] Protected and highly sensitive medical information collected by healthcare entities includes many categories from intimate details of an individual's conditions, symptoms, diagnoses, and treatments to personally identifying information to unique codes which can identify and connect individuals to the

5. Despite professing to value patients' privacy and vowing to protect the confidentiality and security of their private and protected health information, healthcare entities, like Defendants, are collecting, in some instances, "ultra-sensitive personal data" about patients "ranging from those seeking information about their reproductive rights and options, those seeking information regarding their addictions and . . . those seeking mental health counseling."[9]

6. And, while mobile health options have been celebrated as a way to expand treatment options, the tangible, real-world implications and potential for abuse is staggering:

> [T]he sensitive information people share during treatment for substance use disorders could easily impact their employment status, ability to get a home, custody of their children, and even their freedom. Health care providers and lawmakers recognized long ago that the potential threat of losing so much would deter people from getting life-saving help and set up strict laws to protect those who do seek treatment. ***Now, experts worry that data collected on telehealth sites could bring about the harm [the law] was designed to prevent and more, even inadvertently.***[10]

7. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person's personally identifiable

---

collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), https://jezebel.com/the-spooky- loosely-regulated-world-of-online-therapy-1841791137 (last visited May 8, 2023).

[9] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL (June 15, 2022), available at https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (noting that such "personal data can be used in a number of ways. The centers can deliver targeted advertising, on Facebook or elsewhere, aimed at deterring an individual from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive health – targeted at people with similar demographics and interests. And, in the worst-case scenario now contemplated by privacy experts, that digital trail might even be used as evidence against abortion seekers in states where the procedure is outlawed") (last visited May 10, 2023).

[10] *Id.*

protected health information to a third party without express written authorization.

8. In addition, Pennsylvania law provides that "all [medical] records shall be treated as confidential," and that a hospital must receive written authorization of a patient "for release of medical information outside the hospital." 28 Pa. Stat. § 115.27.[8] Further, the Pennsylvania Patient's Bill of Rights provides that "a patient has the right to every consideration of his privacy concerning his own medical care program" and "the right to have all records pertaining to his medical care treated as confidential except as otherwise provided by law or third-party contractual arrangements." 28 Pa. Stat. § 103.22(b)(3-4).

9. Conemaugh "is the largest healthcare provider in west central Pennsylvania, serving over a half-million patients each year through the Conemaugh Physician Group and Medical Staff, a network of hospitals, specialty clinics and patient focused programs. Conemaugh Health System employs over 5,000 clinical and non-clinical staff, and over 450 physicians committed to providing the ideal patient experience." [11]

10. Despite its unique position as a massive and trusted healthcare provider, Conemaugh knowingly configured and implemented into its website, www.conemaugh.org, (the "Website") code-based tracking devices known as "trackers" or "tracking technologies," which collected and transmitted Plaintiffs' and Class Members' Private Information to Facebook, Google, and other third parties, without their knowledge or authorization.

11. Defendants encourage patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to find a doctor,[12] research treatment

[11] About Us, Conemaugh Health System, https://www.conemaugh.org/about (last visited April 13, 2023).
[12] Find a Doctor, Conemaugh Health System, https://www.conemaugh.org/find-a-doctor (last visited Nov. 20, 2023).

options,[13] make an appointment,[14] access the patient portal,[15] pay bills,[16] contact Conemaugh Health System,[17] and more.

12. When Plaintiffs and Class Members used Defendants' Website and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendants embedded tracking technologies from Facebook, Google, DoubleClick, Kenshoo, CallRail, and potentially others, into its Website and Online Platforms, surreptitiously forcing Plaintiffs and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

13. Facebook's tracker is called the Meta Pixel (also referred to as the "Pixel"). The Meta Pixel is a snippet of code, embedded into a website, that tracks information about its visitors and their website interactions.[18] As a visitor uses the website, the Meta Pixel records any "events" it is configured to track, such as pages viewed, buttons clicked, and information submitted.[19] Then, the Pixel transmits the event information back to the website server and to Facebook, where it can be combined with other data and used for marketing.[20]

14. By default, the Meta Pixel tracks information about a website user's device and the

[13] Services, Conemaugh Health System, https://www.conemaugh.org/services (last visited Nov. 20, 2023).
[14] Conemaugh removed online scheduling from its website sometime after June 24, 2022. An archived version of its online scheduling page is available at https://web.archive.org/web/20220624135054/https://www.conemaugh.org/schedule.
[15] Patient Portal, Conemaugh Health System, https://www.conemaugh.org/patient-portal (last visited Nov. 20, 2023).
[16] Online Bill Pay, Conemaugh Health System, https://www.conemaugh.org/pay-my-bill (last visited Nov. 20, 2023).
[17] Contact Us, Conemaugh Health System, https://www.conemaugh.org/contact (last visited Nov. 20, 2023).
[18] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[19] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[20] *Id.*

URLs and domains they visit.[21] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[22] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[23]

15. Operating as designed and as implemented by Defendants, the Meta Pixel allowed Defendants to unlawfully disclose Plaintiffs' and Class Members' private health information, alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendants effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

16. Facebook encourages and recommends that website owners who use the Metal Pixel also employ a Business Tool called Conversions Application Programming Interface ("CAPI").[24]

17. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the

[21] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[22] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[23] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).
[24] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

website user's browser.[25, 26]

18. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[27]

19. Defendants utilized data from these trackers to market its services and bolster their profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

20. The information that Defendants' Meta Pixel and possibly CAPI sent to Facebook included Private Information that Plaintiffs and Class Members submitted to Defendants' Website, including Plaintiffs' and Class Members' (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) appointment requests; (5) desired locations or facilities where treatment was sought; and (6) phrases and search queries (such as searches for symptoms, treatment options, or types of providers) conducted via the general search bar.

21. Such information allows third parties (e.g., Facebook) to learn that a particular

[25] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).
[26] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).
[27] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers, who then target Plaintiffs and Class Members with online advertisements, based on the information they communicated to Defendants via the Website. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

22. In addition to the Facebook tracker and likely CAPI, Defendants installed other tracking technologies, including Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail. On information and belief, these trackers operate similarly to the Meta Pixel and transmitted Plaintiffs' and Class Members' Private Information to unauthorized third parties.

23. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue—without their consent.

24. Neither Plaintiffs nor any Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook, Google, DoubleClick, Kenshoo, CallRail, or any other third parties uninvolved in their treatment.

25. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into its Website and servers, Conemaugh did not disclose to Plaintiffs or Class Members that it was sharing their sensitive and confidential communications and Private Information with third parties including Facebook, Google, DoubleClick, Kenshoo, CallRail, and possibly others.

26. Defendants further made express and implied promises to protect Plaintiffs' and

Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendants, including in its privacy policies and elsewhere.

27. Defendants owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and Private Information safe, secure, and confidential.

28. Upon information and belief, Conemaugh utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

29. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard their information from unauthorized disclosure.

30. Defendants breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, DoubleClick, Kenshoo, and CallRail; (v) failing to protect Private Information and take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

31. As a result of Defendants' conduct, Plaintiffs and Class Members have suffered

numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of the Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.

32. Plaintiffs seek to remedy these harms and bring causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Invasion of Privacy; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Fiduciary Duty; (VII) Violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Stat. §§ 5701., *et seq.*; (VIII) Violation of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1); (IX) Breach of Confidence; and (X) Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. §§ 201-1, *et seq*.

PARTIES

33. Plaintiff TACEY HABERKORN is a natural person and a resident and citizen of Pennsylvania, where she intends to remain. She is a patient of Conemaugh and a victim of Defendants' unauthorized Disclosure of Private Information.

34. Plaintiff JANE DOE is a natural person and a resident and citizen of Pennsylvania, where she intends to remain, with a principal residence in Johnstown in Cambria County. She is a patient of Conemaugh and a victim of Defendants' unauthorized Disclosure of Private Information.

35. Defendant Duke Lifepoint Healthcare, LLC is a joint venture between Duke Health and LifePoint Health that was established in 2011.

36. Defendant DLP Healthcare, LLC is a Delaware limited liability company with a principal place of business located at 330 Seven Springs Way, Brentwood, Tennessee 37027.

37. Defendant DLP Conemaugh Memorial Medical Center, LLC, is a Delaware limited liability company with its principal place of business in the Commonwealth of Pennsylvania at 1086

Franklin Steet, Johnstown, Pennsylvania 15905 in Cambria County.

38. Defendant DLP Physician Practices, LLC, is a Delaware limited liability company with its principal place of business at 1111 Franklin Street, Suite 300, Johnstown, Pennsylvania 15905 in Cambria County.

39. Defendant DLP Conemaugh JV, LLC is a Delaware limited liability company principal place of business located at 330 Seven Springs Way, Brentwood, Tennessee 37027.

40. Defendant DLP Conemaugh Holding Company, LLC, is a Delaware limited liability company principal place of business located at 330 Seven Springs Way, Brentwood, Tennessee 37027.

41. Defendants John Doe 1-5 are entities that, separately or in conjunction with the other Defendants names herein, own, operate, and/or control the website www.conemaugh.org and the information disclosed by patients of the Conemaugh Health System to the Website. The names and identities of John Doe 1-5 are currently unknown and are within the exclusive control of Defendants and their agents.

42. Defendants Duke LifePoint Healthcare, LLC; DLP Healthcare, LLC; DLP Conemaugh Memorial Medical Center, LLC; DLP Physician Practices, LLC; DLP Conemaugh Holding Company, LLC; DLP Conemaugh JV, LLC; and John Does 1-5 are referred to collectively herein as "Conemaugh" or "Defendants."

COMMON FACTUAL ALLEGATIONS

A. Background

43. Conemaugh "is the largest healthcare provider in west central Pennsylvania, serving over a half-million patients each year through the Conemaugh Physician Group and Medical Staff, a network of hospitals, specialty clinics and patient focused programs. Conemaugh Health System

employs over 5,000 clinical and non-clinical staff, and over 450 physicians committed to providing the ideal patient experience."[28]

44. Conemaugh operates four hospitals, Conemaugh Memorial Medical Center, Conemaugh Meyersdale Medical Center, Conemaugh Miners Medical Center, Conemaugh Nason Medical Center, and three outpatient centers, Conemaugh East Hills, Conemaugh Ebensburg, and Conemaugh Somerset.[29]

45. Conemaugh serves many of its patients via its Website and Online Platforms, which it encourages patients to find a doctor,[30] research treatment options,[31] make an appointment,[32] access the patient portal,[33] pay bills,[34] contact Conemaugh Health System,[35] and more.

46. To enhance its marketing efforts and increase profits, Defendants purposely installed the Meta Pixel and other trackers onto its Website to gather Private Information about Plaintiffs and Class Members. But Defendants did not only generate information for its own use: it also shared patient Private Information, including that belonging to Plaintiffs and Class Members, with Facebook, Google, DoubleClick, Kenshoo, CallRail, and potentially other unauthorized third parties.

---

[28] About Us, Conemaugh Health System, https://www.conemaugh.org/about (last visited April 13, 2023).
[29] Locations, Conemaugh Health System, https://www.conemaugh.org/locations (last visited Nov. 20, 2023).
[30] Find a Doctor, Conemaugh Health System, https://www.conemaugh.org/find-a-doctor (last visited Nov. 20, 2023).
[31] Services, Conemaugh Health System, https://www.conemaugh.org/services (last visited Nov. 20, 2023).
[32] Conemaugh removed online scheduling from its website sometime after June 24, 2022. An archived version of its online scheduling page is available at https://web.archive.org/web/20220624135054/https://www.conemaugh.org/schedule.
[33] Patient Portal, Conemaugh Health System, https://www.conemaugh.org/patient-portal (last visited Nov. 20, 2023).
[34] Online Bill Pay, Conemaugh Health System, https://www.conemaugh.org/pay-my-bill (last visited Nov. 20, 2023).
[35] Contact Us, Conemaugh Health System, https://www.conemaugh.org/contact (last visited Nov. 20, 2023).

47. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

48. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[36]

49. In conjunction with its advertising business, Facebook encourages website owners like Defendants to use its "Business Tools" to gather customer data, identify customers and potential customers, and market products and services.

50. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

51. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[37] Businesses that want to target customers and advertise their services can also create their own tracking parameters by building a "custom event."[38]

52. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[39] When an individual accesses a webpage that is hosting the Meta Pixel, the

[36] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).
[37] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).
[38] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.
[39] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

53. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy.

54. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[40].

55. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[41]

56. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values

[40] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[41] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

unless you include them as part of Advanced Matching or optional values.[42]

57. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.

- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[43]

58. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendants' method of transmitting Plaintiffs' and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

59. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

60. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

61. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP

[42] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[43] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

Responses, along with corresponding cookies.[44]

62. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

63. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

64. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

65. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

66. In this way, the Meta Pixel acts much like a traditional wiretap, intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

67. Separate from the Meta Pixel, Facebook and other third parties place cookies in the web browsers of users who visit their websites or online platforms. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to identify users of a Meta-Pixel-enabled

[44]"Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

68. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[45] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

69. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[46] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website server(s), in accordance with Facebook's documentation.

70. The Meta Pixel, Conversions API, and other third-party trackers do not provide any

[45] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).
[46] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

71. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, Google, or others.

72. In this case, Defendants employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

73. Consequently, when Plaintiffs and Class Members visited Defendants' Website and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

74. Conemaugh also employed trackers from Google, DoubleClick, Kenshoo, and CallRail. On information and belief, Defendants likewise transmitted Plaintiffs' and the Class Members' Private Information to these third parties without Plaintiffs' and Class Members' knowledge or authorization.

iii. Defendants' Privacy Policies Prohibit the Use and Disclosure of Private Information without Authorization

75. Conemaugh is covered under its Notice of Privacy Practices[47] and its Online Privacy Policy,[48] which are posted and maintained on Defendants' Website (collectively referred

[47] Notice of Privacy Practices, Conemaugh Health System https://web.archive.org/web/20230402032657/https://www.conemaugh.org/sites/conemaugh/assets/uploads/Patient%20Privacy%20Practices%20rev.%202023.pdf (link archived April 2, 2023), **attached hereto as Exhibit B.**

[48] Online Privacy Policy, Conemaugh Health System, https://web.archive.org/web/20230402233548/https://www.conemaugh.org/privacy-policy (link archived April 2, 2023), **attached hereto as Exhibit C.**

to as "Privacy Policies").

76. Defendants' Notice of Privacy Practices provides: "This notice applies to all Conemaugh Health System facilities and affiliates" and "describes how medical information about you may be used and disclosed and how you can get access to this information."[49]

77. The Notice of Privacy Practices further states, "**In these cases we never share your information unless you give us written permission:** • Marketing purposes. • Sale of your information . . . ." [50]

78. Therein, Defendants further acknowledge, represent, and promise:

> **Our Responsibilities**
>
> • We are required by law to maintain the privacy and security of your protected health information.
>
> • We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
>
> • We must follow the duties and privacy practices described in this notice and give you a copy of it.
>
> • We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.[51]

79. Further, Conemaugh's Online Privacy Policy[52] provides:

> This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal information that you submit to us when you submit a Contact Us form, attach a resume, and browse our website.
>
> […]

[49] Exhibit B, Notice of Privacy Practices, *supra*.
[50] *Id.*
[51] *Id.*
[52] Exhibit C, Online Privacy Policy, *supra.*

> We've designed our public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information").[53]

80. Conemaugh's Online Privacy Policy goes on to say:

> Personal information can be anything you've provided through our public websites that identifies you. For example: Your name, email address, and street address are types of personal information. We store this information behind a complex series of firewalls, in a way that maximizes security and confidentiality.[54]

81. Defendants' Online Privacy Policy promises that:

- We will only use the information to provide you with the services you have requested and as otherwise described in this Public Online Privacy Policy.
- We will NOT sell, rent, or license the personal information you provide within our public websites.
- We do NOT provide any personally identifiable information about our users to any third party.
- Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.[55]

82. Defendants' Online Privacy Policy goes on to say:

> We use "cookies" to personalize our site for you and to collect aggregate information about site usage by all of our users. A cookie is a text file that our website transfers to your computer's hard drive for record keeping purposes. The cookie assigns a random, unique number to your computer. **It does not contain information that would personally identify you.**[56]

iv. Defendants Unlawfully Disclosed Plaintiffs' and Class Members' Private Information

83. Despite these representations in its Privacy Policies, Defendants did, in fact, disclose Private Information to third parties for marketing purposes.

84. Through their use of the Meta Pixel, Defendants disclosed to Facebook Plaintiff and Class Members' Private Information communicated via its Website, including Plaintiff and

[53] *Id.*
[54] *Id.*
[55] *Id.* (emphasis in original).
[56] *Id.* (emphasis added).

Class Members' (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) appointment requests; (5) desired locations or facilities where treatment was sought; and (6) phrases and search queries (such as searches for symptoms, treatment options, or types of providers) conducted via the general search bar.

85. An example illustrates the point. If a patient uses conemaugh.org to book an appointment with a cardiologist, Defendants' Website directs them to communicate Private Information. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendants' Pixel, including the medical condition the patient types into the search bar and the filters they select.

86. In the example below, the user typed "I have hypertension" into the search bar, and then used the filtering tools to identify a "Female" physician who speaks "English," is specialized in "Cardiology," and is currently "Accepting New Patients."

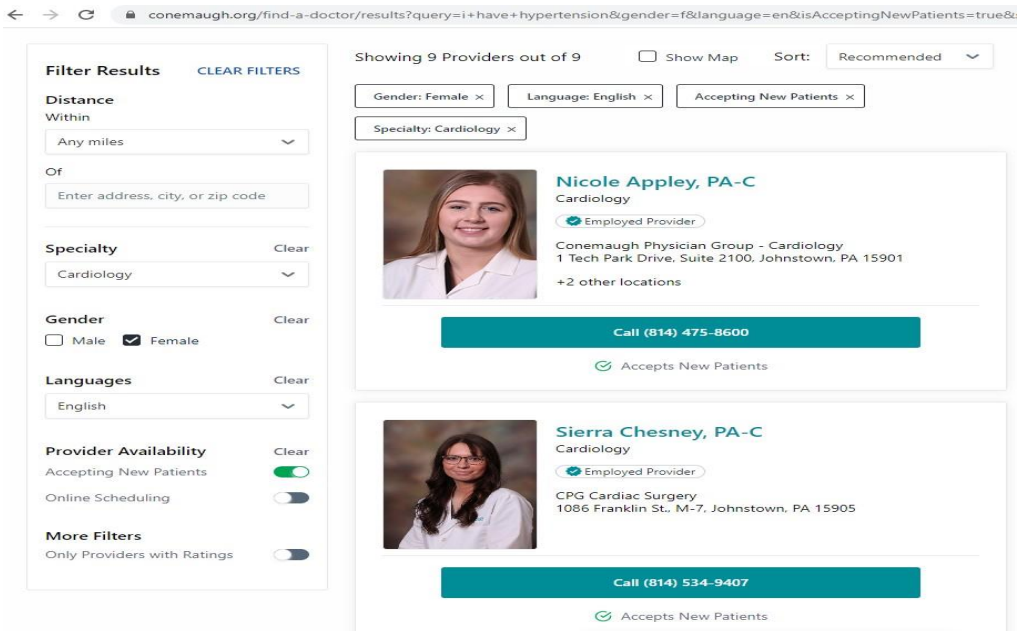


Figure 2. Screenshot taken from conemaugh.org as the user searches for a cardiologist and communicates information via the search bar and filtering tools.

87. Unbeknownst to ordinary patients, this particular webpage—which, as noted in the

HHS Bulletin, is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendants' Pixel. The image below shows the "behind the scenes" portion of the Website that is invisible to ordinary users. Importantly, each entry in the right-hand column represents just one instance in which Defendants' Pixel or other tracking technologies sent this particular user's information to third parties like Facebook.

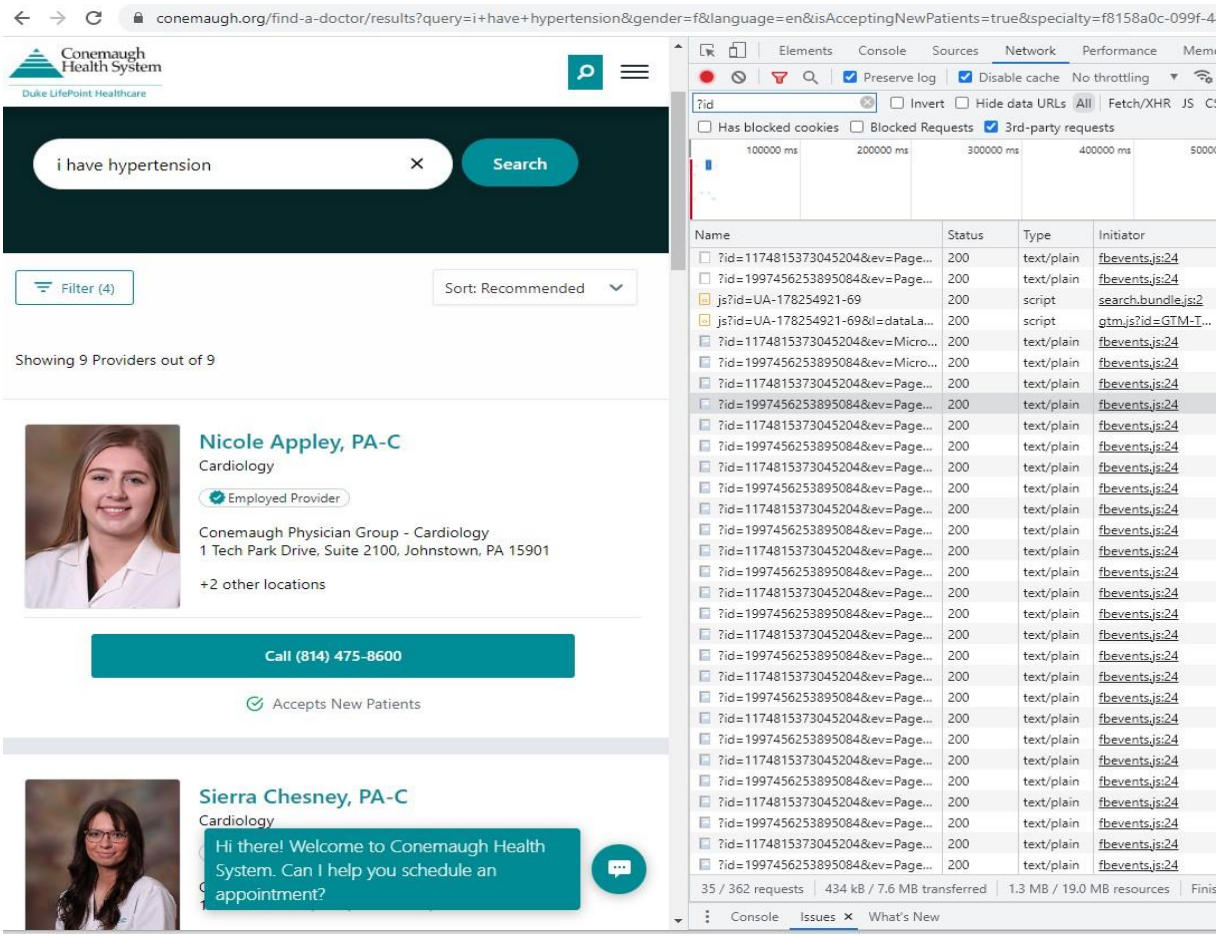


Figure 3. Screenshot taken from conemaugh.org which shows the mark-up (user-facing portion of the website) alongside the network traffic. Each entry in the column to the right represents just one instance in which the user's information was transmitted to Facebook via Defendants' Pixel.

88. Thus, without alerting the user, Defendants' Pixel sends each and every communication the user made via the webpage to Facebook, and the images below confirm that the communications Defendants send to Facebook contain the user's Private Information,

including in the descriptive URL that shows the "I have hypertension" search.

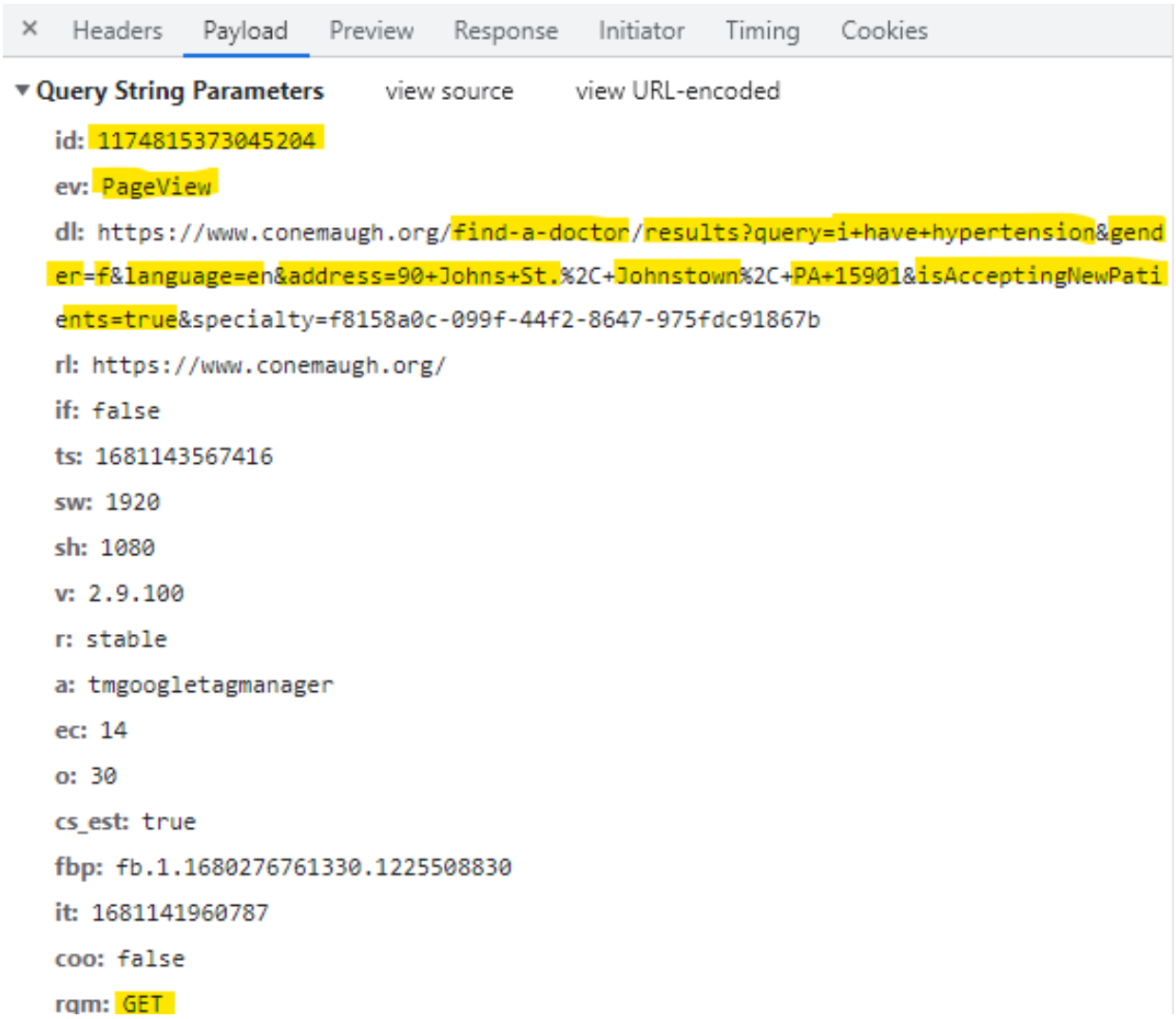


Figure 4. Screenshot taken from user's network traffic report during their physician search.

89. The image above shows what information is sent to Facebook when the user continues their search by typing their address into the distance filter. The first line of highlighted text, "id:1174815373045204," refers to Defendants' Pixel ID and confirms that Defendants have embedded the Pixel into the source code for this particular webpage.

90. The second line of text, "ev: PageView," identifies and categorizes which actions the user took on the webpage ("ev:" is an abbreviation for event, and "PageView" is the type of

event). Thus, this identifies the user as having viewed the particular webpage after applying their search criteria, and it also identifies them as having requested the content from Defendants via the user's GET Request.

91. The next lines of highlighted text show Defendants have disclosed to Facebook that the user: (1) is a patient seeking medical care from Defendants via www.conemaugh.org; (2) in conjunction with a specific medical condition (highlighted above as "query=i+have+hypertension"); and (3) is in the process of booking an appointment or searching for a particular physician ("find-a-doctor") who is female "gender=f," speaks English "language=en," and is accepting new patients "isAcceptingNewPatients=true." The exact address the user communicated is also transmitted to Facebook, "address=90+Johns+St . . . Johnstown . . . PA+15901."

92. If a patient searches for their cardiologist by name, that physician's name and specialty is also transmitted to Facebook as shown in the images below.

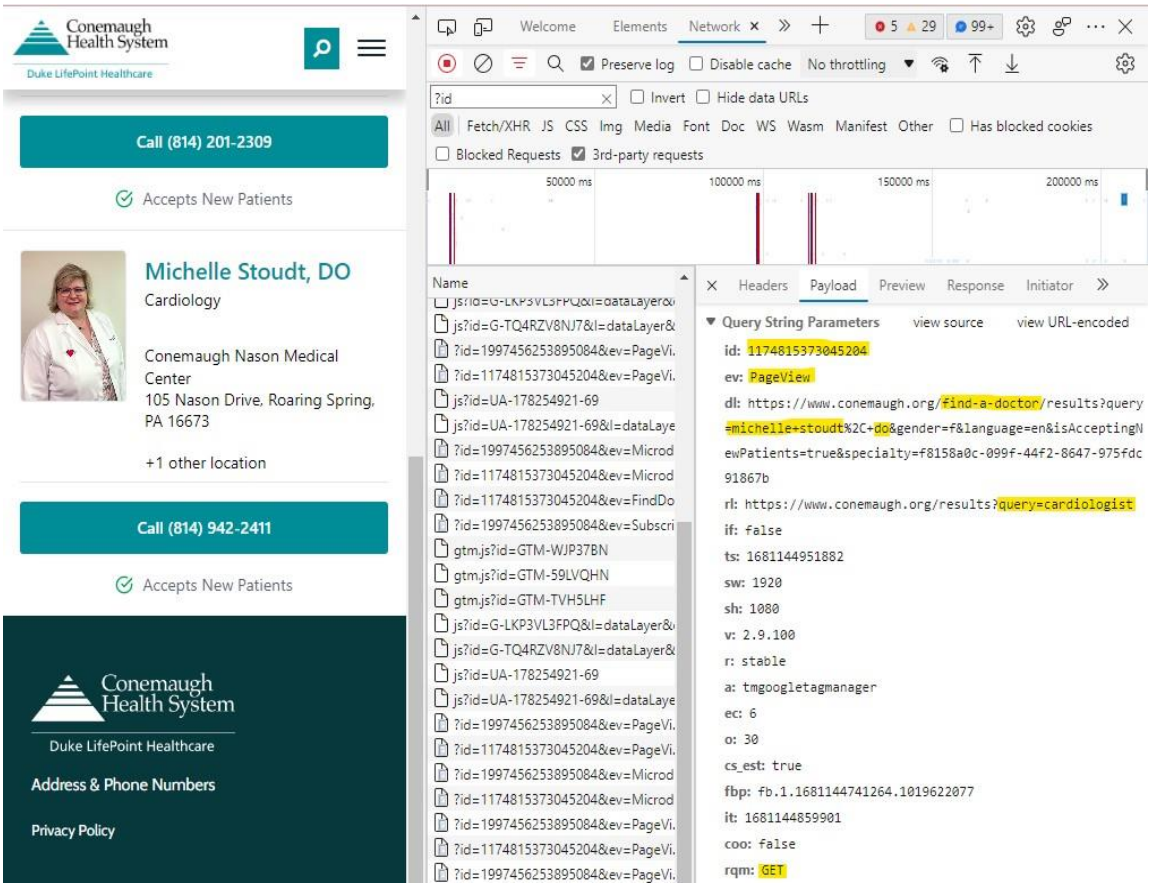


Figure 5. Screenshot that includes the user's network traffic alongside the mark-up for this particular webpage.

93. The highlighted text reveals the identity of the user's physician or prospective physician (highlighted above as "michelle+stoudt . . . do"), and the physician's particular field of medicine or specialty "query=cardiologist."

94. Importantly, each time the user's communications are transmitted to Facebook, Facebook receives them alongside the user's Facebook ID (highlighted as "c_user=" in the images below) thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.[57]

[57] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiffs have redacted the corresponding string of numbers to preserve the user's anonymity.

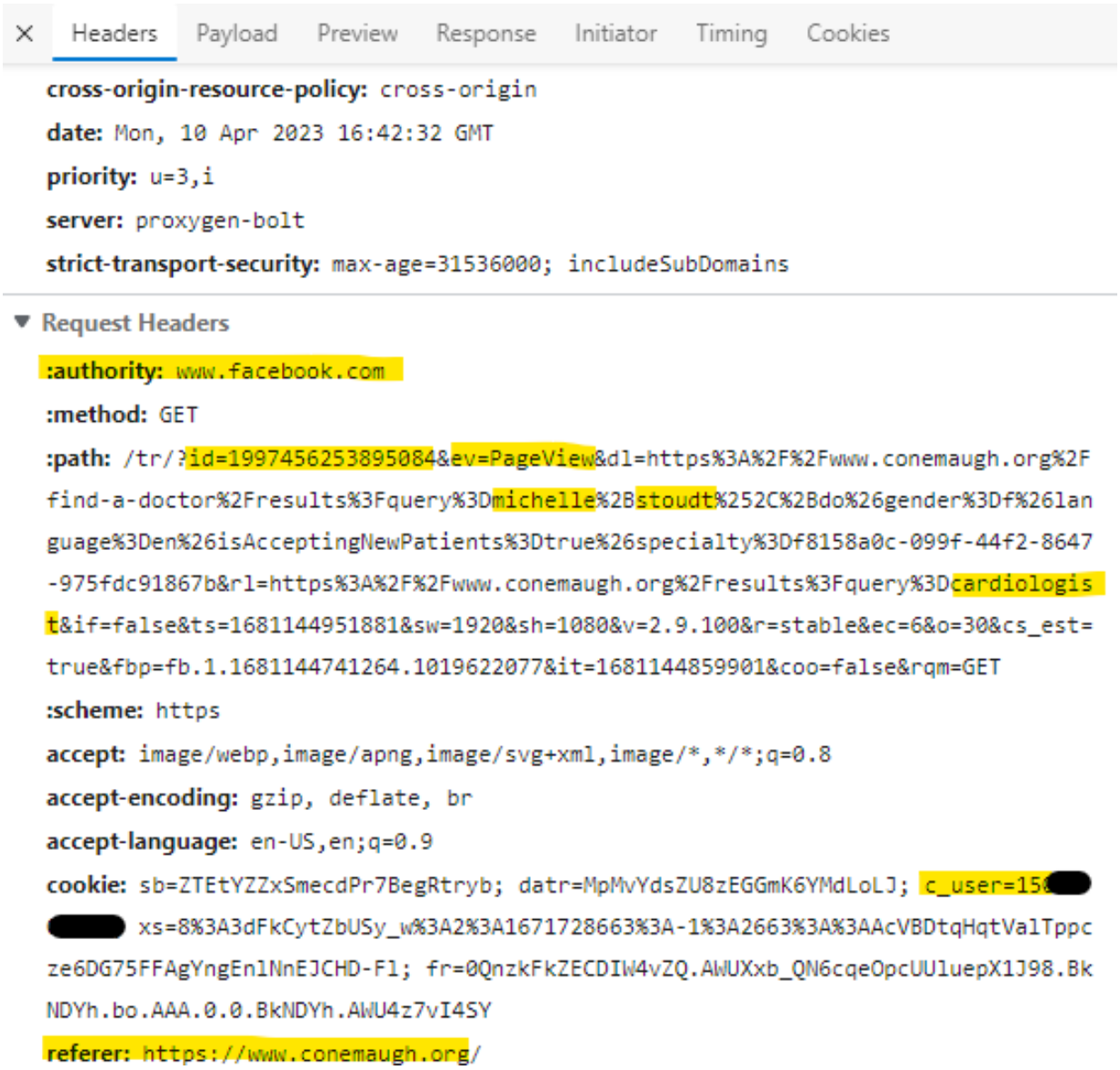


Figure 6. Screenshot of the user's network traffic depicting the user's URL Request headers associated with Defendants' Pixel ID 1997456253895084.

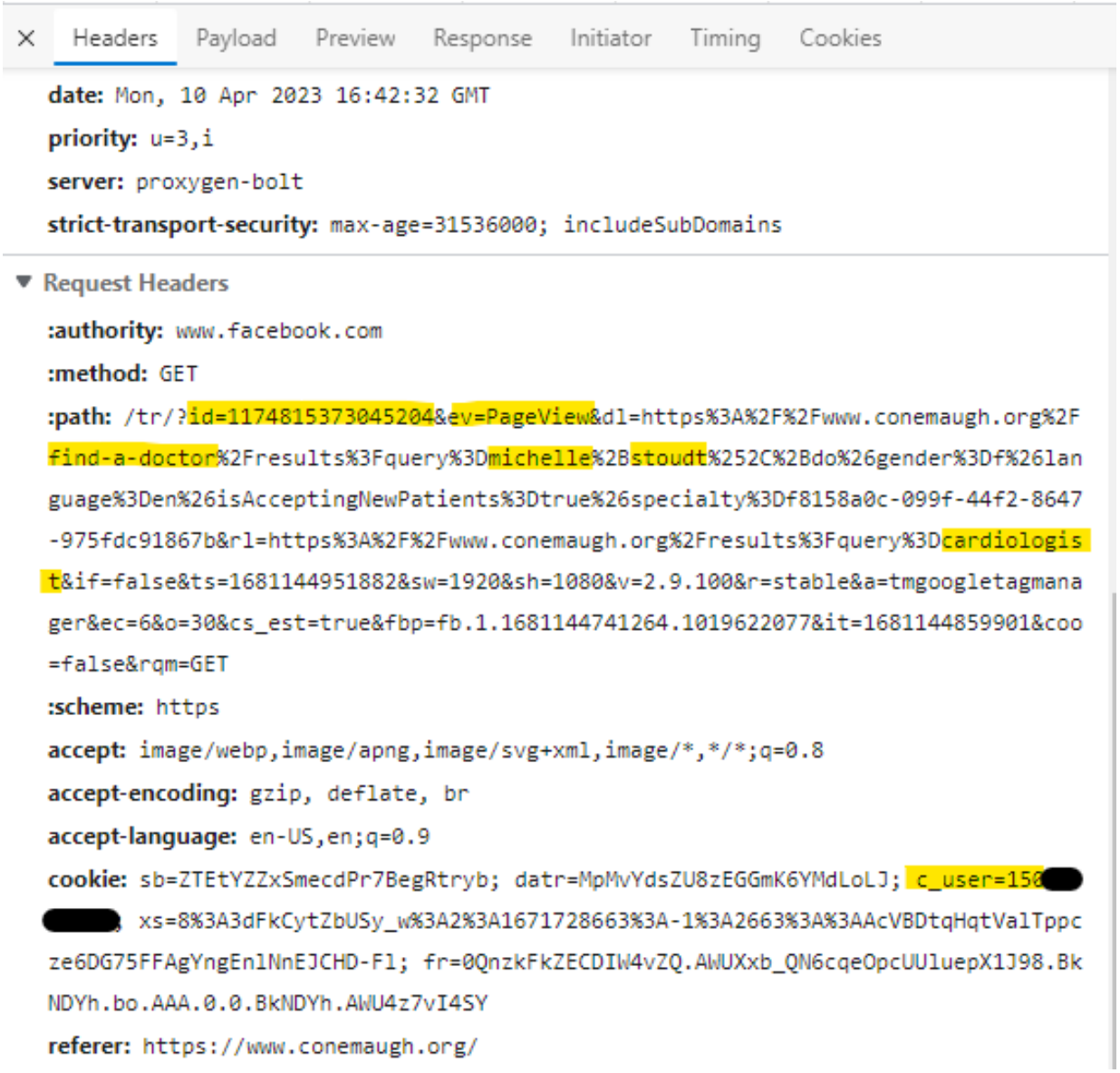


Figure 7. Screenshot of the user's network traffic depicting the user's URL Request headers associated with Defendants' Pixel ID 1174815373045204.

95. Although the images above appear to be identical, they represent two distinct transmissions of the user's communications and interactions on Defendants' Website. The first transmission is attributed to Pixel ID 1997456253895084, and the second transmission is attributed to Pixel ID 1174815373045204. In each instance, Facebook receives the transmission alongside the user's c_user ID, thereby uniquely identifying the individual and matching the communication

and underlying data with their unique Facebook account.

96. Defendants' ability to control and manipulate the Pixel is made evident by their use of custom events. For example, in the image below, Defendants have created a custom event that is coded and transmitted to Facebook as "ev: FindDoctor." Thus, in addition to default events like "SubscribedButtonClicks" and "PageViews," Defendants are actively broadcasting the fact that the individual user is seeking medical care via the Website.

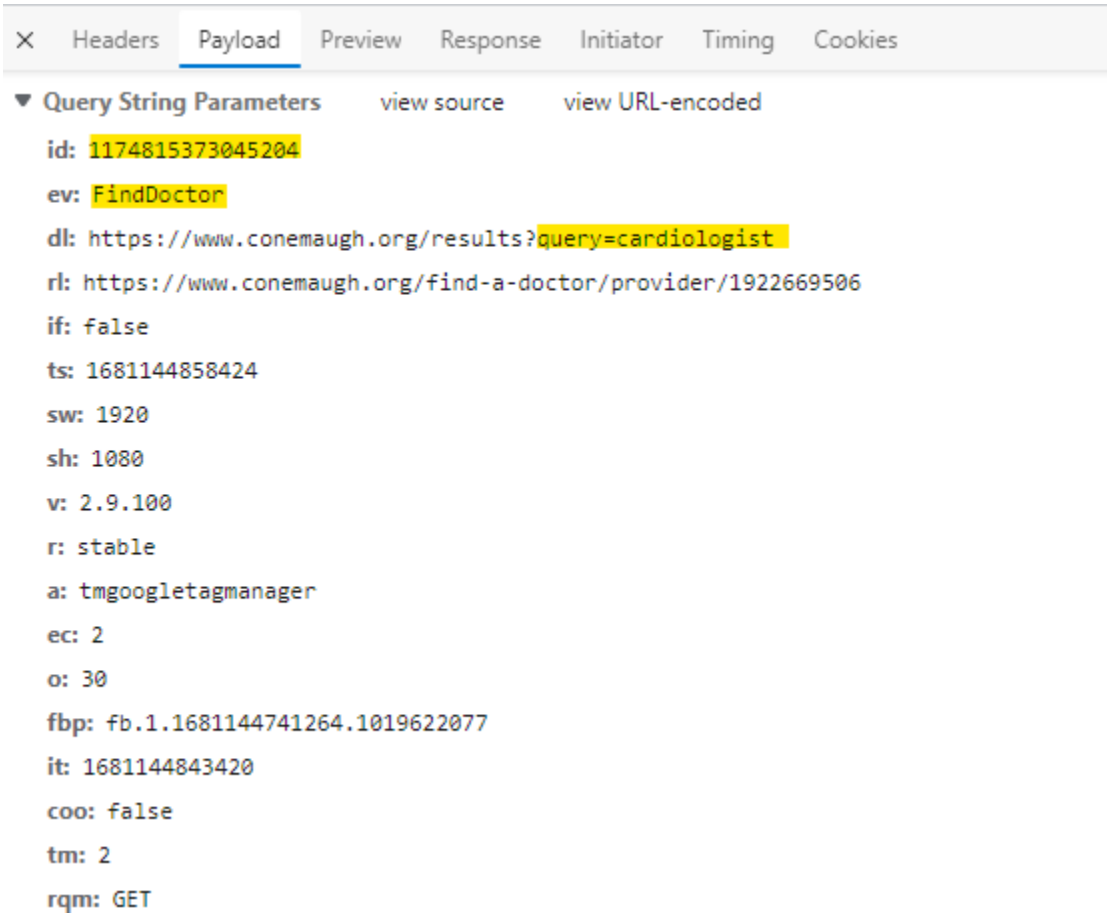


Figure 8. Screenshot taken from the user's network traffic report showing that Defendants have created custom events using the Facebook Pixel.

97. To make matters worse, Defendants track, transmit, and disclose the exact text and phrases their patients type into the general search bar on the homepage, conemaugh.org.

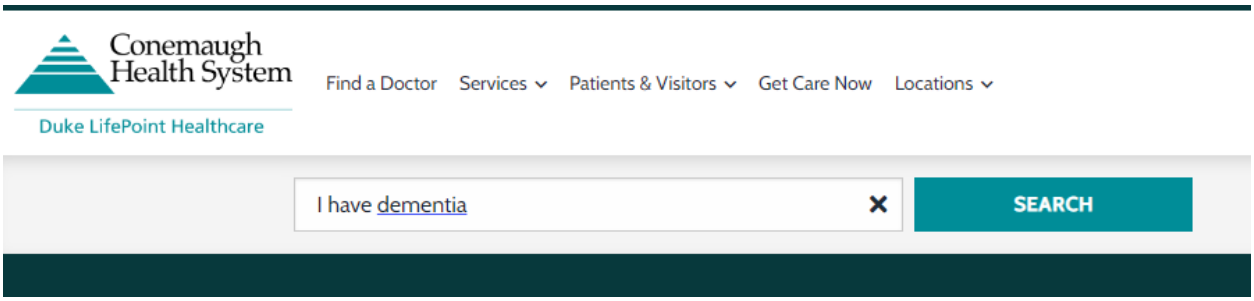
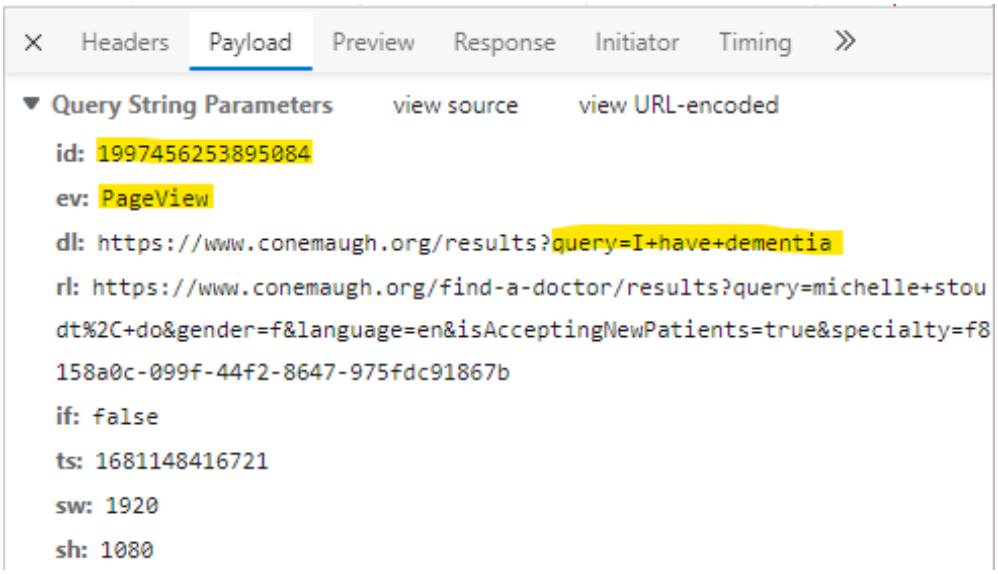


Figure 9. Screenshot taken when the user types "I have dementia" into the general search bar on Defendants' homepage.

98. In the example above, the user typed "I have dementia" into the search bar, and Defendants' Pixel sent that exact phrase to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. This is simply unacceptable, and there is no legitimate reason for sending this information to Facebook.

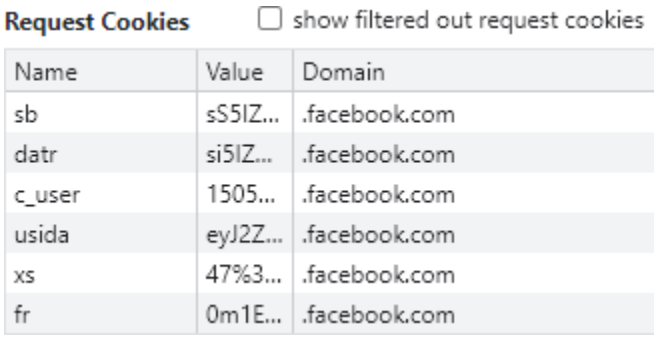


Figures 10 & 11. Screenshots taken from the user's traffic report depicting the "Payload" and corresponding "Headers" associated with the user's online activity and communications to Defendants.

99. In each of the examples above, the user's Website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third parties to identify individual website users,

but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the Website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

100. Facebook receives at least six cookies when Defendants' Website transmits information via the Pixel:

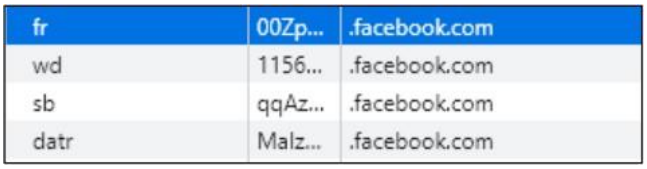


Request Cookies ☐ show filtered out request cookies

Name	Value	Domain
sb	sS5IZ...	.facebook.com
datr	si5IZ...	.facebook.com
c_user	1505...	.facebook.com
usida	eyJ2Z...	.facebook.com
xs	47%3...	.facebook.com
fr	0m1E...	.facebook.com

Figure 12.

101. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:[58]



fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 13.

102. The fr cookie contains an encrypted Facebook ID and browser identifier.[59] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay

[58] The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[59] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 11, 2023).

on a user's website browser for up to 90 days *after* the user has logged out of Facebook.[60]

103. The cookies listed above in figures 12 and 13 are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendants are ultimately responsible for the manner in which individual Website users were identified via these cookies, and Facebook would not have received this data but for Defendants' implementation and use of the Pixel throughout their website.

104. Defendants also revealed Website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user:[61]

_fbp	fb.1.1681149483157.865798246	.conemaugh.org

Figure 14.

105. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e. a cookie that was created and placed on the Website by Defendants.[62]

106. The Meta Pixel uses both first- and third-party cookies.

107. After receiving this information from Defendants, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond

[60] *Cookies & other storage technologies*, FACEBOOK https://www.facebook.com/policy/cookies/ (last visited May 11, 2023).

[61] *Id.*

[62] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

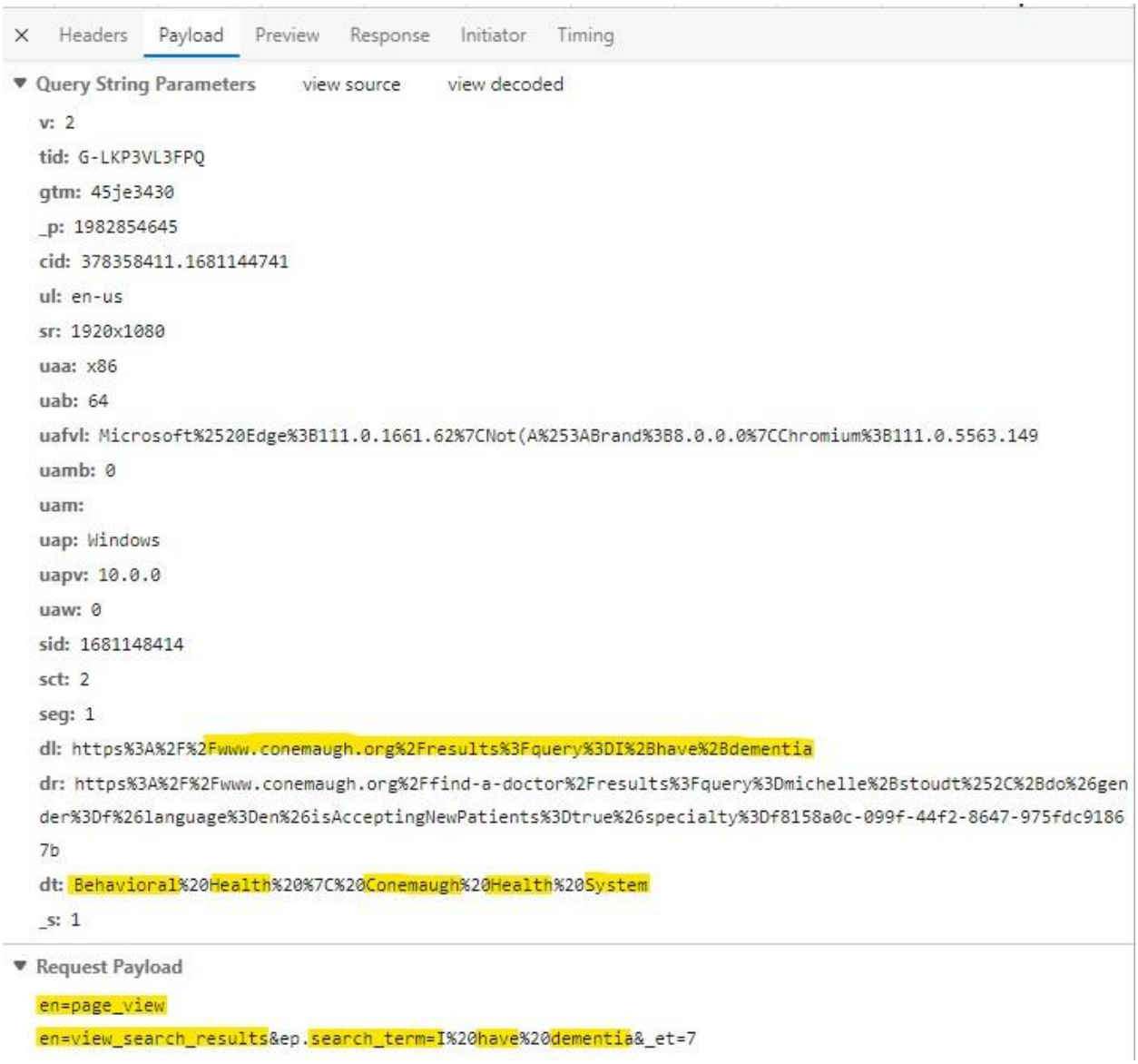
to your ad."[63] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[64] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[65] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[66]

108. Google and other companies process data in a similar manner and use it to build marketing and other data profiles allowing for targeted online advertising.

109. Defendants also use Google Tag Manager, Google Tag Manager, DoubleClick, Kenshoo, and CallRail to track Plaintiff and Class Members' private communications and transmit that information to unauthorized third parties.

110. For example, the images below indicate that Defendants are also sending patients' protected health information to Google via the Google Analytics tool and Google Tag Manager. Both images below contain the user's search phrase ("I have dementia"), and Defendants do not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in either image below.

[63] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[64] *Id.*
[65] *Id.*
[66] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).



× Headers Payload Preview Response Initiator Timing

▼ Query String Parameters view source view decoded

v: 2
tid: G-LKP3VL3FPQ
gtm: 45je3430
_p: 1982854645
cid: 378358411.1681144741
ul: en-us
sr: 1920x1080
uaa: x86
uab: 64
uafvl: Microsoft%2520Edge%3B111.0.1661.62%7CNot(A%253ABrand%3B8.0.0.0%7CChromium%3B111.0.5563.149
uamb: 0
uam:
uap: Windows
uapv: 10.0.0
uaw: 0
sid: 1681148414
sct: 2
seg: 1
dl: https%3A%2F%2Fwww.conemaugh.org%2Fresults%3Fquery%3DI%2Bhave%2Bdementia
dr: https%3A%2F%2Fwww.conemaugh.org%2Ffind-a-doctor%2Fresults%3Fquery%3Dmichelle%2Bstoudt%252C%2Bdo%26gender%3Df%26language%3Den%26isAcceptingNewPatients%3Dtrue%26specialty%3Df8158a0c-099f-44f2-8647-975fdc91867b
dt: Behavioral%20Health%20%7C%20Conemaugh%20Health%20System
_s: 1

▼ Request Payload

en=page_view
en=view_search_results&ep.search_term=I%20have%20dementia&_et=7

Figures 15 & 16. The screenshots above were captured from the user's network report and depict what types of information Google received. Notably, the user was executing their search through the Microsoft Edge web browser, not the Google Chrome browser. Stated differently, Google would not have received this information but for Defendants' use of Google's analytics tools.

111. Defendants' use of the Google Analytics tool causes Google to receive patients' communications searching for specific medical conditions alongside the patients' IP address, which (as noted in the HHS Bulletin) is also impermissible under HIPAA.

112. Additionally, upon information and belief and as described above, Defendants also installed and used Facebook's Conversions API tool when it implemented the Pixel because: (1) the Pixel is automatically programmed to function via both first-party and third-party cookies;

and (2) Conversions API works in conjunction with the Pixel and other Facebook Business Tools to transmit information to Facebook.

113. While the third-party cookies described above allow Facebook to match information to a specific individual, the Conversions API tool and first-party cookies Defendants installed record, store, and transmit users' communications and Private Information directly to Facebook even when the user has blocked or disabled third-party cookies in their web browser.

114. These "server to server" communications cannot be accessed by Plaintiffs because they are not transmitted via the web user's browser and do not otherwise rely on third-party cookies to facilitate the transmission of data.

115. Defendants could have chosen not to use the Meta Pixel, or it could have configured it to limit the information that it communicated to Facebook, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiffs' and Class Members' Private Information.

116. Along those same lines, Defendants could have chosen not to use Google Tag Manager, Google Tag Manager, DoubleClick, Kenshoo, and CallRail to track Plaintiffs and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers despite the harm to Plaintiffs' and Class Members' privacy.

117. Defendants used and disclosed Plaintiffs' and Class Members' Private Information to unauthorized third parties for the purpose of marketing its services and increasing its profits.

118. On information and belief, Defendants shared, traded, or sold Plaintiff and Class Members' Private Information with Facebook, Google, DoubleClick, Kenshoo, and CallRail in exchange for improved targeting and marketing services.

119. Plaintiffs did not consent, agree, authorize, or otherwise permit Defendants to disclose their Private Information for marketing purposes. Defendants did not notify Plaintiffs and Class Members of their practice of disclosing patients' Private Information to Facebook, Google, DoubleClick, Kenshoo and CallRail; nor did Defendants provide any means of opting out of these disclosures. Defendants, nonetheless, used Plaintiffs' and Class Members' Private Information and knowingly disclosed that Private Information to unauthorized entities for Defendants' own gain.

120. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

121. Defendants misrepresented that they would preserve the security and privacy of Plaintiffs' and Class Members' Private Information, while it knowingly disclosed their Private Information to unauthorized third parties.

122. By law, Plaintiffs and the Class Members are entitled to privacy in their Private Information and confidential communications. Conemaugh deprived Plaintiffs and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff and Class Members' confidential communications and Private Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook, Google, DoubleClick, Kenshoo, and CallRail; (3) profited from the Disclosure; and (4) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

Plaintiff Tacey Haberkorn

123. Plaintiff Haberkorn has been a patient of Conemaugh since 2021 and has received healthcare services from Conemaugh and physicians in Conemaugh's network.

124. Plaintiff Haberkorn relied on Conemaugh's Website and Online Platforms to communicate confidential patient information. She used Defendants' Website frequently and regularly between 2021 and 2022.

125. Plaintiff Haberkorn has been a Facebook user since 2009.

126. On numerous occasions, Plaintiff Haberkorn accessed Defendants' Website on her phone. Plaintiff used the Website to search for specific doctors and specialists who could help with her specific medical conditions. She also used Defendants' Online Platforms to schedule appointments, check her medical records and test results, and fill out medical forms.

127. Plaintiff Haberkorn accessed Defendants' Website to receive healthcare services from Defendants or Defendants' affiliates, at Defendants' direction, and with Defendants' encouragement.

128. Plaintiff Haberkorn reasonably expected that her online communications with Conemaugh were confidential, solely between herself and Conemaugh, and that, as such, those communications would not be transmitted to or intercepted by a third party.

129. Plaintiff Haberkorn provided her Private Information to Defendants and trusted that the information would be safeguarded according to Conemaugh's privacy policies and the law.

130. Through its use of the Meta Pixel, Defendants disclosed to Facebook

a. Plaintiff Haberkorn's identity;

b. Plaintiff Haberkorn's status as a patient;

c. Plaintiff Haberkorn's seeking of medical treatment;

d. Plaintiff Haberkorn's health conditions and the treatment she sought; and

e. when Plaintiff Haberkorn accessed Defendants' patient portal.

131. By failing to receive the requisite consent to disclose Plaintiff Haberkorn's Private Information, Conemaugh violated its agreements with Plaintiff Haberkorn, its own policies, and the law.

132. Since using Defendants' Website, Plaintiff Haberkorn has been targeted by online advertisements directed towards her medical conditions.

133. Plaintiff Haberkorn paid for Defendants' healthcare services, which included reasonable privacy and data security protections for her Private Information; however, Plaintiff Haberkorn did not receive the privacy and security protections for which she paid.

134. Because of Defendants' Disclosure, Plaintiff Haberkorn has suffered injuries, including monetary damages; loss of privacy; unauthorized disclosure of her Private Information; unauthorized access to her Private Information by third parties; use of her Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of her Private Information; lost benefit of her bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of her information.

Plaintiff Jane Doe

135. Plaintiff Doe is a patient of Conemaugh and has received healthcare services from Conemaugh and physicians in Conemaugh's network for health conditions including asthma, anxiety, pregnancy, and polyps. Plaintiff Doe has received treatment at the Conemaugh Memorial Medical Center, 1086 Franklin Street, Johnstown, Pennsylvania, and Conemaugh East Hills Outpatient Center, 1450 Scalp Avenue, Suite 1000, Johnstown, Pennsylvania.

136. Plaintiff Doe relied on Conemaugh's Website and Online Platforms to communicate confidential patient information. Plaintiff Doe accessed the website regularly and frequently during the time Defendants had the Meta Pixel and other trackers enabled on its Website. On numerous occasions, Plaintiff Doe has used Defendants' Website and Online Platforms to find clinic locations, find primary care physicians, check test results, communicate with physicians, and confirm appointments.

137. Plaintiff Doe accessed Defendants' Website to receive healthcare services from Defendants or Defendants' affiliates, at Defendants' direction, and with Defendants' encouragement.

138. Plaintiff Doe reasonably expected that her online communications with Conemaugh were confidential, solely between herself and Conemaugh, and that, as such, those communications would not be transmitted to or intercepted by a third party.

139. Plaintiff Doe provided her Private Information to Defendants and trusted that the information would be safeguarded according to Conemaugh's privacy policies and the law.

140. Through its use of the Meta Pixel, Defendants disclosed to Facebook

a. Plaintiff Doe's identity;

b. Plaintiff Doe's status as a patient;

c. Plaintiff Doe's seeking of medical treatment;

d. Plaintiff Doe's health conditions and the treatment she sought; and

e. when Plaintiff Doe accessed Defendants' patient portal.

141. By failing to receive the requisite consent to disclose Plaintiff Doe Private Information, Conemaugh violated its agreements with Plaintiff Doe, its own policies, and the law.

142. Since using Defendants' Website, Plaintiff Doe has been targeted by online

advertisements directed towards her medical conditions.

143. Plaintiff Doe paid for Defendants' healthcare services, which included reasonable privacy and data security protections for her Private Information; however, Plaintiff Doe did not receive the privacy and security protections for which she paid.

144. Because of Defendants' Disclosure, Plaintiff Doe has suffered injuries, including monetary damages; loss of privacy; unauthorized disclosure of her Private Information; unauthorized access to her Private Information by third parties; use of her Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of her Private Information; lost benefit of her bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of her information.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

145. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[67] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

146. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on

[67] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[68]

147. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[69] When a user was having their period or informed the app of their intention to get pregnant, Flo would inform Facebook, which could then use the data for targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[70]

148. More recently, Facebook employees admitted to lax protections for sensitive user data. In 2021, Facebook engineers on the ad business product team conceded "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[71]

---

[68] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[69] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[70] *Id.*
[71] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

149. In June 2022, an investigation by The Markup[72] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[73] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[74] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[75]

150. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also patients' names, addresses, email addresses, and phone numbers.[76]

151. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[77]

152. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply

[72] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[73] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*

troubled" by what the hospitals capturing and sharing patient data in this way.[78]

D. Defendants Violated HIPAA Standards

153. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[79]

154. Guidance from the U.S. Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

155. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[80]

156. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis

[78] *Id.*
[79] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[80] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

added).[81]

157. In addition, HHS's Office for Civil Rights (OCR) issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[82]

158. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[83]

159. The HHS Bulletin notes that such information—even when sent to an "unauthenticated webpage" (*i.e.*, a webpage that does not require users to log in before accessing the webpage) —constitutes a disclosure of PHI to the tracking technology vendor.[84]

160. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to

[81] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.
[82] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.
[83] *Id.*
[84] U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.

> others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.[85]

161. In other words, HHS has expressly stated that Defendants' conduct of implementing the Meta Pixel violates HIPAA Rules.

E. Defendants Violated FTC Standards, and the FTC and HHS Have Taken Action

162. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[86]

163. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[87]

164. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[88] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you

---

[85] *Id.* (emphasis in original) (internal citations omitted).
[86] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **Exhibit A.**
[87] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.
[88] *Id.*

do not use the information obtained through use of a tracking technology for any marketing purposes."[89]

165. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[90]

166. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[91]

167. As such, the FTC and HHS have expressly stated that conduct like Defendants' runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

---

[89] *Id.*

[90] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

[91] *See, e.g.*, U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; U.S. v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

F. Defendants Violated Pennsylvania Law

168. Pennsylvania law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

169. All patient medical records "shall be treated as confidential." 28 Pa. Stat. § 115.27. In addition, a hospital must receive written authorization of a patient "for release of medical information outside the hospital." *Id.*[92]

170. Further, the Pennsylvania Patient's Bill of Rights provides that "a patient has the right to every consideration of his privacy concerning his own medical care program" and "the right to have all records pertaining to his medical care treated as confidential except as otherwise provided by law or third-party contractual arrangements." 28 Pa. Stat. § 103.22(b)(3-4).

171. Defendants' actions described herein violated Pennsylvania law.

172. Defendants' violations of Pennsylvania law regarding the privacy and confidentiality of medical treatment and records provide context for the elements of Plaintiff's and Class Members' underlying claims, including, *inter alia*, (1) the confidential nature of the information communicated to Defendants; (2) Plaintiffs' and Class Members' reasonable expectation of privacy in their confidential Private Information; (3) the highly offensive nature of Defendants' disclosure of Private Information; and (4) the fact that the Private Information communicated (including searches for specific symptoms, health conditions, or doctors or the scheduling of appointments) constitutes the "contents" of the communication.

[92] Pennsylvania law also states that "medical records are the property of the hospital" but that "they shall not be removed from the hospital premises except for court purposes" and that copies may only be made available "for authorized appropriate purposes such as insurance claims, and physician review, consistent with § 115.27 (relating to confidentiality of medical records)." 28 Pa. Stat. §115.28.

G. Defendants Violated Industry Standards

173. A medical provider's duty of confidentiality is a cardinal rule, embedded in doctor-patient and hospital-patient relationships.

174. The American Medical Association's ("AMA") Code of Medical Ethics requires the protection of patient privacy and communications, and these rules are applicable to Conemaugh and its physicians.

175. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

176. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

177. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiffs' and Class Members' Expectation of Privacy

178. At all times when Plaintiffs and Class Members provided their Private Information to Defendants, they had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for a commercial

marketing and sales purposes, unrelated to patient care.

179. Plaintiffs and Class Members would not have used Defendants' Website or Online Platforms and shared their Private Information if they had known Defendants would disclose that Private Information to third parties and/or aid third parties in intercepting that Private Information.

I. IP Addresses are Personally Identifiable Information

180. Defendants also disclosed Plaintiffs' and Class Members' IP addresses to Facebook, Google, DoubleClick, Kenshoo, and CallRail, through its use of the Meta Pixel and other tracking technologies.

181. An IP address is a number that identifies the address of a device connected to the Internet.

182. IP addresses are used to identify and route communications on the Internet.

183. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

184. Facebook tracks every IP address ever associated with a Facebook user.

185. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

186. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code," specifically listing IP addresses as an example of PII. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

187. Consequently, by disclosing IP addresses, Defendants' business practices violated HIPAA and industry privacy standards.

J. Defendants were Enriched and Benefitted from the Use of Trackers and Unauthorized Disclosures

188. The sole purpose for Defendants' use of the Meta Pixel and other tracking technology was to enhance its marketing efforts and increase its profits.

189. In exchange for disclosing the Private Information of its patients, Defendants were compensated by Facebook, Google, and likely others in the form of enhanced advertising services and more cost-efficient marketing.

190. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendants re-targeted patients and potential patients.

191. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendants.

K. Plaintiffs' and Class Members' Private Information Had Financial Value

192. The data concerning Plaintiffs and Class Members, collected and shared by Defendants, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[93] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain

[93] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).

online content.[94] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[95]

193. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[96]

194. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

195. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, it described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[97]

196. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who

---

[94] *Id.*
[95] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).
[96] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).
[97] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.

compile the data from providers and other health-care organizations and sell it to buyers."[98]

197. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[99]

198. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

199. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

200. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

---

[98] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

[99] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/. (last visited Sep. 1, 2023).

201. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[100]

TOLLING, CONCEALMENT, AND ESTOPPEL

202. The applicable statutes of limitation have been tolled as a result of Conemaugh's knowing and active concealment and denial of the facts alleged herein.

203. Conemaugh seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing patients with no indication that their Website usage was being tracked and transmitted to third parties. Conemaugh knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiffs and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, Google, DoubleClick, Kenshoo, and CallRail.

204. Even while exercising due diligence, Plaintiffs and Class Members could not have discovered the full scope of Conemaugh's conduct, because there were no disclosures or other indications that they were interacting with websites employing Meta Pixel or any other tracking technology.

205. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Conemaugh's illegal interception and disclosure of Plaintiffs' Private Information has continued unabated through at least May 18, 2023. What is more, Conemaugh was under a duty to disclose the nature and significance of their data collection practices but did not do so. Conemaugh is therefore, is estopped from relying on any statute of limitations defenses.

[100] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

CLASS ALLEGATIONS

206. Plaintiffs bring this class action on behalf of themselves and on behalf of other similarly situated persons.

207. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and other tracking technologies without authorization.

In the alternative, Plaintiffs seek to represent a "Pennsylvania Class" defined as

> All individuals residing in Pennsylvania who are, or were, patients of Defendants or any of their affiliates, used Defendants' Website, and had their Private Information disclosed to a third party without authorization or consent.

The Nationwide Class and Pennsylvania Class are collectively referred to as the "Class."

208. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, and any entity in which any of the Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

209. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

210. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendants, and the Class is identifiable within Defendants' records.

211. Ascertainability. Class Members are readily identifiable from information in Defendants' possession, custody, and control.

212. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendants had a duty to protect Plaintiffs' and Class Members' Private Information;

b. whether Defendants had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. whether Defendants failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. whether Defendants failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendants' conduct amounts to negligence *per se*;

j. whether Defendants committed invasion of privacy;

k. whether Defendants breached its contract with Plaintiffs and the Class Members; or in the alternate, whether Defendants were unjustly enriched; and,

l. whether Defendants breached fiduciary duties to Plaintiffs and the Class Members.

m. whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information.

213. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendants' use and incorporation of Meta Pixel and other tracking technology.

214. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

215. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have suffered is typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

216. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

217. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged. If the class action device were not used, Defendants would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

218. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

219. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

220. Unless a Class-wide injunction is issued, Defendants may continue in its unlawful use and disclosure of Class Members' Private Information; failure to properly secure the Private Information of Class Members; and refusal to provide proper notification to and obtain proper consent from Class Members.

221. Further, Defendants has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

222. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to

a. whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. whether Defendants breached the implied contract;

f. in the alternate, whether Defendants were unjustly enriched;

g. whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been used and disclosed to third parties;

h. whether Defendants failed to implement and maintain reasonable security procedures and practices;

i. whether Defendants committed an invasion of privacy;

j. whether Defendants had fiduciary duties to Plaintiffs and the Class Members;

k. whether Defendants breached its fiduciary duties; and,

l. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information; and

m. whether Plaintiffs and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

223. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

224. Defendants owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using Plaintiffs' and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

225. Defendants acted with wanton and reckless disregard for the privacy and

confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendants.

226. Defendants owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' disclosure of their Private Information to benefit third parties and Defendants. Defendants actively sought and obtained Plaintiffs' and Class Members' Private Information.

227. Private Information is highly valuable, and Defendants knew, or should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendants by way of data harvesting, advertising, and increased sales.

228. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiffs and Class Members. This failure actually and proximately caused Plaintiffs' and Class Members' injuries.

229. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

230. Defendants' breach of its common-law duties to exercise reasonable care proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages,

including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' negligence. These injuries are ongoing, imminent, immediate, and continuing.

231. In failing to secure Plaintiffs' and Class Members' Private Information, PII and PHI, Defendants are guilty of oppression, fraud, or malice. Defendants acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of herself and the Class.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

232. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

233. Plaintiffs allege this negligence *per se* theory as an alternative to their other negligence claim.

234. Pursuant to the laws set forth herein, 28 Pa. Stat. § 115.27, 28 Pa. Stat. § 103.22, the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

235. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

236. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII and PHI.

237. Defendants owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

238. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, Google, and others gaining access to Plaintiffs' and Class Members' PII and PHI, and resulting in Defendants' liability under principles of negligence *per se*.

239. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

240. Plaintiffs' and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendants' negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

241. As a proximate result of Defendants' negligence and breach of duties as set forth above, Defendants' breaches of duty caused Plaintiffs and Class Members to, *inter alia*, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their PII and PHI, diminution in the value of their personal data for which

there is a tangible value, and/or a loss of control over their PII and PHI, all of which constitute actionable actual damages.

242. In failing to secure Plaintiffs' and Class Members' PII and PHI, Defendants are guilty of oppression, fraud, or malice. Defendants acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of herself and the Class.

243. Defendants' conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' PII and PHI, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendants' conduct. Plaintiffs and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendants' negligence *per se*.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

244. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

245. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via its Website and Online Platforms.

246. Plaintiffs and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendants to receive and that they understood Defendants would keep private.

247. As described herein, Defendants' installed tracking technologies like the Meta Pixel on Defendants' Website and Online Platforms which surreptitiously commandeered Plaintiffs' and Class Members' web browsers and forced Plaintiffs' and Class Members' web

browsers to duplicate their communications with Defendants and send them to third parties such as Facebook.

248. Defendants' use of technology to effectively plant a bug on Plaintiffs' and Class Members' web browsers and force the disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion in their private affairs and concerns.

249. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendants' representations and Privacy Policies. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI coupled with PII is highly offensive to the reasonable person.

250. As a result of Defendants' actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

251. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

252. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

253. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter

Defendants from engaging in such conduct in the future.

254. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

255. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

256. As a condition of receiving medical care from Defendants, Plaintiffs and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiffs and Class Members entered into implied-in-fact contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

257. Implicit in the agreement between Conemaugh and its patients, Plaintiffs and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

258. Conemaugh had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Conemaugh.

259. Conemaugh had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and to notify them of any breach of that information.

260. Additionally, Conemaugh implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

261. Plaintiffs and Class Members fully performed their obligations under the implied

contract with Conemaugh, but Defendants did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Conemaugh in the absence of their implied contracts with Conemaugh that their Private Information would be kept in confidence and would instead have retained the opportunity to control their Private Information for uses other than receiving medical treatment from Conemaugh.

262. Conemaugh breached the implied contracts with Plaintiffs and Class members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties and failing to notify them of the breach of that Private Information.

263. Conemaugh's acts and omissions have materially affected the intended purpose of the implied contracts that required Plaintiffs and Class Members to provide their Private Information in exchange for medical treatment and benefits.

264. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

265. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

266. Plaintiffs re-allege and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

267. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claim.

268. Plaintiffs and Class Members conferred a monetary benefit upon Conemaugh in the form of valuable sensitive medical information that Defendants collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiffs and the Class Members conferred a benefit on Defendants in the form of monetary compensation.

269. Plaintiffs and Class Members would not have used Conemaugh's services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose their Private Information to third parties.

270. Conemaugh appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

271. As a result of Conemaugh's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

272. The benefits that Defendants derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendants to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

273. Conemaugh should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

274. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

275. A relationship existed between Plaintiffs and the Class, on the one hand, and Defendants, on the other, in which Plaintiffs and the Class put their trust in Defendants to protect the Private Information of Plaintiffs and the Class, and Defendants accepted that trust.

276. Defendants breached the fiduciary duty that it owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty; failing to act with the highest and finest loyalty; and failing to protect and, indeed, intentionally disclosing, their Private Information.

277. Defendants' breach of fiduciary duty was a legal cause of injury-in-fact and damages to Plaintiffs and the Class.

278. But for Defendants' breach of fiduciary duty, the injury-in-fact and damages to Plaintiffs and the Class would not have occurred.

279. Defendants' breach of fiduciary duty substantially contributed to the injury and damages to the Plaintiffs and the Class.

280. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VII
VIOLATION OF THE PENNSYLVANIA WIRETAPPING & ELECTRONIC SURVEILLANCE CONTROL ACT, 18 Pa. Stat. §§ 5701, *et seq*.
(On Behalf of Plaintiffs and the Class)

281. Plaintiffs re-allege and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

152. The Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") is codified at 18 Pa. Stat. §§ 5701, *et seq*.

153. 18 Pa. Stat. § 5725 provides, in pertinent part, as follows:

> (a) Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person: (1) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher; (2) Punitive damages. (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

154. WESCA defines "person" as any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. 18 Pa. Stat. § 5702.

155. Defendants each constitute a "person" under WESCA, 18 Pa. Stat. § 5702.

156. WESCA prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. 18 Pa. Stat. §§ 5701, 5703(1).

157. WESCA defines "intercept," as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Stat. § 5702.

158. WESCA also prohibits the disclosure of, or use of, the contents of any wire, electronic, or oral communication, or any evidence derived therefrom, with knowledge that the information was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Stat. § 5703(2)-(3).

159. WESCA further prohibits the knowing access without authorization of a facility through which an electronic communication is provided or exceeds an authorization to access

that facility and obtains, or alters access to a wire or electronic communication while that communication is in electronic storage. 18 Pa. Stat. § 5741(a)

160. WESCA is also violated where, for the purpose of commercial advantage or private commercial gain, a person knowingly accesses without authorization a facility through which an electronic communication service is provided, or exceed access to that facility, and obtains access to a wire or electronic communication while that communication is in electronic storage. 18 Pa. Stat. § 5741

161. As set forth herein, Defendants knowingly, willfully, and intentionally intercepted and disclosed Plaintiffs' and Class Members' electronic communications, without the consent of the Plaintiffs and Class Members, using Facebook's tracking devices, Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail.

162. Defendants knowingly, willfully, and intentionally intercepted Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to third parties including Facebook, Google, DoubleClick, Kenshoo, and CallRail without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

163. The devices used in this case, include, but are not limited to

a. those to which Plaintiffs' and Class Members' communications were disclosed;

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on Defendants' Website and/or server;

h. Defendants' computer servers;

i. third-party source code utilized by Defendants; and

j. computer servers of third parties (including Facebook, Google, Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail).

164. Defendants aided in the interception of communications between Plaintiffs and Class Members and Defendants that were redirected to and recorded by third parties without the Plaintiffs' or Class Members' consent.

165. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed, or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. Stat. § 5725(a).

282. As a result of Defendants' violations of WESCA, pursuant to 18 Pa. Stat. § 5725(a), Plaintiffs and the Class Members are entitled to recover actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VIII
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2511(1), *et seq*.
(On Behalf of Plaintiffs and the Class)

283. Plaintiffs re-allege and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

284. The ECPA protects both sending and receipt of communications.

285. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

286. The transmissions of Plaintiffs' Private Information to Defendants via Defendants' Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

287. The transmissions of Plaintiffs' Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

288. **Electronic Communications**. The transmission of Private Information between Plaintiffs and Class Members and Defendants via their Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

289. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

290. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

166. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the

meaning of 18 U.S.C. § 2510(5):

a. those to which Plaintiffs' and Class Members' communications were disclosed;

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on Defendants' Website and/or server;

h. Defendants' computer servers;

i. third-party source code utilized by Defendants; and

j. computer servers of third parties (including Facebook, Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail).

291. Whenever Plaintiffs and Class Members interacted with Defendants' Website, Defendants, through the Meta Pixel and other tracking technologies embedded on their Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

292. Whenever Plaintiffs and Class Members interacted with Defendants' Website, Defendants, through the Meta Pixel and other tracking technologies embedded on their Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and

Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

167. Whenever Plaintiffs and Class Members interacted with Defendants' Website, Defendants, through the source code embedded on their web properties, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

293. Defendants' intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

294. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C.

295. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

296. Defendants intentionally used the wire or electronic communications to increase their profit margins. Defendants specifically used the Pixel, and likely other third party tracking

technologies, to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

297. Defendants were not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

298. Plaintiffs and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

299. Any purported consent that Defendants received from Plaintiffs and Class Members was not valid.

300. **Unauthorized Purpose**. Defendants intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, the Pennsylvania Patient's Bill of Rights, Pennsylvania confidentiality of medical records statute, and invasion of privacy, among others.

301. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

302. Defendants are a "party to the communication" with respect to patient communications. However, Defendants' simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

303. Defendants' acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Pennsylvania, including

a. criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. criminal violation of Pennsylvania Computer Crime statutes, including: Unlawful use of computer (18 Pa. Stat. §7611); Unlawful duplication (18 Pa. Stat. §7614); and Computer trespass (18 Pa. Stat. §7615);

c. violation of the Pennsylvania Patient's Bill of Rights, 28 Pa. Stat. §§103.22;

d. violation of Pennsylvania statute regarding the confidentiality of medical records, 28 Pa. Stat.§ 115.27;

e. violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. §§ 201-1, *et seq.*; and

f. invasion of Privacy.

168. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

304. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

305. Defendants' conduct violated 42 U.S.C. § 1320d-6 in that it

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Facebook, Google, Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail, without patient authorization.

306. Defendants' conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendants' use of the Facebook, Google, DoubleClick, Kenshoo, and CallRail

source code was for Defendants' commercial advantage to increase revenue from existing patients and gain new patients.

307. Under 18 Pa. Stat. § 7611, a person commits the offense of unlawful use of a computer if he

a. accesses or exceeds authorization to access, alters, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof with the intent to interrupt the normal functioning of a person or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;

b. intentionally and without authorization accesses or exceeds authorization to access, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof; or

c. intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network, computer database, World Wide Web site or telecommunication device.

308. Defendants violated the 18 Pa. Stat. §7611 in that

a. Defendants accessed and exceeded authorization to access Plaintiffs' and Class Members' computing devices and data as part of a deception and without their

authorization, including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communications with Defendants simultaneously to Defendants and Facebook, Google, and others; and

b. Defendants intentionally or knowingly and without authorization gave or published confidential information about Plaintiffs' and Class Members' computer or telecommunication device to third parties.

309. Under 18 Pa. Stat. § 7614, a person commits the offense of unlawful duplication if he makes or causes to be made an unauthorized copy, in any form, including but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by or produced by a computer or computer network.

310. Defendants violated 18 Pa. Stat. §7614 by exceeding their authorization to access Plaintiffs' and Class Members' computers including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to make unauthorized copies of Plaintiffs' and Class Members' electronic data and to send identifiers and the content of communications with Defendants simultaneously to Defendants and Facebook, Google, and others.

311. Under 18 Pa. Stat. §7615, a person commits the offense of computer trespass if he knowingly and without authority or in excess of given authority uses a computer or computer network with the intent to

a. temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network; or

b. alter or erase any computer data, computer programs or computer software.

312. Defendants violated 18 Pa. Stat. §7615 when it knowingly and without Plaintiffs' or Class Members' authorization inserted the fbp, ga, and gid cookies on Plaintiffs' and Class Members' computing devices.

313. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendants to Google, Facebook, and others.

314. Defendants knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendants to Google, Facebook, and others.

315. Under the Pennsylvania Patient's Bill of Rights, 28 Pa. Stat. § 103.22, a patient has the right to every consideration of his privacy concerning his own medical care program. 28 Pa. Stat. § 103.22(b)(3). In addition, a patient has the right to have all records pertaining to his medical care treated as confidential except as otherwise provided by law or third-party contractual arrangements. 28 Pa. Stat. § 103.22(b)(4).

316. Defendants violated the Pennsylvania Patient's Bill of Rights by disclosing Plaintiffs' and Class Members' Private Information to third parties without authorization or consent.

317. Under 28 Pa. Stat. § 115.27, all medical records must be treated as confidential. A hospital must receive written authorization of a patient for release of medical information outside the hospital.

318. Under 28 Pa. Stat. § 115.28, medical records are the property of the hospital and shall not be removed from the hospital premises except for court purposes. Copies may only be made available for authorized appropriate purposes such as insurance claims, and physician

review, consistent with § 115.27 (relating to confidentiality).

319. Defendants violated 28 Pa. Stat. §§ 115.27-28 by failing to treat Plaintiffs' and Class Members' medical records as confidential and by disclosing those records to third parties outside the hospital without written authorization or consent and without an authorized appropriate purpose. Increasing Defendants' revenues through enhanced marketing and advertising and online targeting is not an authorized appropriate purpose.

320. Defendants are not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their individually-identifiable patient health information on their Website, because they used their participation in these communications to improperly share Plaintiffs' and Class Members' individually-identifiable patient health information with Facebook and Google, third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their individually-identifiable patient health information, and that Plaintiffs and Class Members did not consent to receive this information.

321. Defendants accessed, obtained, and disclosed Plaintiffs' and Class Members' Private Information for the purpose of committing the crimes and torts described herein because they would not have been able to obtain the information or the marketing services if it had complied with the law.

322. As such, Defendants cannot viably claim any exception to ECPA liability.

323. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendants' invasion of privacy in the following ways.

a. Defendants have intruded upon, intercepted, transmitted, shared, and used Plaintiffs' and Class Members' individually-identifiable patient health

information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes, which has caused Plaintiffs and the Class Members to suffer a loss of privacy and emotional distress.

b. Defendants received substantial financial benefits from their use of Plaintiffs' and Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiffs or the Class Members.

c. Defendants received substantial, quantifiable value from their use of Plaintiffs' and Class Members' individually-identifiable patient health information, such as understanding how people use their website and determining what ads people see on their website, without providing any value or benefit to Plaintiffs or the Class Members.

d. Defendants have failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information.

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendants making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

324. As a result of Defendants' violation of the ECPA, Plaintiffs are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory

and punitive damages, and attorney's fees and costs.

COUNT IX
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

325. Plaintiffs re-allege and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

326. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information, as recently affirmed in *Opris v. Sincera Reprod. Med.*, CV 21-3072, 2022 WL 1639417, at *11 (E.D. Pa. May 24, 2022)*; see also Burger v. Blair Medical Assoc., Inc.*, 600 Pa. 194, 204, 964 A.2d 374, 380 (2009) ("The duty on a health care facility's part to maintain the confidentiality of medical records arises out of the confidential nature of the relationship and the personal nature of the information which must be disclosed in the ordinary course of medical treatment.").

327. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendants, including communications exchanged on Defendants' Website.

328. Contrary to their duties as a medical provider and their express promises of confidentiality, Defendants installed their Pixel and Conversions API to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendants, including Private Information and the contents of such information.

329. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

330. The third-party recipients included, but may not be limited to, Facebook, Google, and Google Analytics, Google Tag Manager, DoubleClick, Kenshoo, and CallRail.

331. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

332. As a direct and proximate cause of Defendants' unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendants' breach in that

a. sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendants eroded the essential confidential nature of the provider-patient relationship;

d. general damages for invasion of their rights in an amount to be determined by a jury;

e. nominal damages for each independent violation;

f. Defendants took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality;

h. Defendants' actions diminished the value of Plaintiffs' and Class Members' Private Information; and

i. Defendants' actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT X
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. §§ 201-1, *et seq.*
(On Behalf of Plaintiffs and the Class

333. Plaintiffs re-allege and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

334. Plaintiff, the members of the Class, and Defendants are all "persons" within the meaning of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa. Stat. § 201-2(2).

335. The UTPCPL prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

336. Under the UTPCPL, "[u]nfair or deceptive acts or practices" include: "[r]epresenting that… services have sponsorship, approval, characteristics, . . . [or] benefits . . . that they do not have," 73 Pa. Stat. § 201-2(4)(v); "[r]epresenting that… services are of a particular standard . . . [or] quality . . . if they are of another," *id.* § 201-2(4)(vii); "[a]dvertising… services with intent not to sell them as advertised," *id.* § 201-2(4)(ix); and "[e]ngaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding," *id.* § 201-2(4)(xxi).

337. Defendants' acts, practices, and omissions alleged in this Complaint constitute unlawful, unfair, and deceptive acts and practices under the UTPCPL.

338. Defendants knew or should have known about the unauthorized disclosure of Plaintiffs' and the Class's Private Information via the Meta Pixel, yet Defendants concealed that information from Plaintiffs and the Class.

339. Defendants engaged in unlawful, unfair, and deceptive acts and practices prohibited by the UTPCPL by, among other things, misrepresenting or omitting material facts to Plaintiffs and the Class regarding the adequacy of Defendants' protection of their Private Information, in violation of 73 Pa. Stat. §§ 201-(4)(v), (vii), (ix), and (xxi);

340. Defendants' acts and omissions and its misrepresentations were intentional, knowing, and undertaken to mislead the public, including Plaintiffs and the members of the Class.

341. Defendants' unfair and deceptive acts include but are not limited to the following.

a. Defendants encouraged patients to use its Website and Online Platforms while representing its commitment to protecting the privacy of the Private Information. At the same time, Conemaugh was disclosing Plaintiffs' and Class Members' Private Information to Facebook, Google, and others, without Plaintiffs' or Class Members' knowledge, consent, or authorization.

b. Defendants also promised patients that it will never sell their medical information without patients' written authorization. Meanwhile, they were exchanging Plaintiffs' and Class Members' Private Information with Facebook, Google, and other third-parties in exchange for enhanced marketing services.

c. Furthermore, Defendants represented that they would never use Plaintiffs' and Class Members' Private Information for marketing purposes without express authorization from Plaintiffs and Class Members. Still, they used Plaintiffs' and Class Members' Private Information for the purpose of developing marketing profiles and advertising its services online.

d. Finally, Defendants claimed that the information they tracked via its Website did not contain personally identifying information. In fact, Defendants used the Meta

Pixel and other tracking technologies to track Plaintiffs' and Class Members' IP addresses, device and browser information, and third-party cookies—information more than sufficient to personally identify Plaintiffs and Class Members.

342. Defendants' unlawful, unfair, and deceptive acts and practices were unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury to Plaintiffs and members of the Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

343. Defendants possessed exclusive knowledge about the disclosure of Plaintiffs' and the Class Member's Private Information to unauthorized parties via the Meta Pixel to their detriment.

344. Defendants had a duty to disclose the foregoing to Plaintiffs and members of the Class and failed to do so.

345. Plaintiffs and members of the Class reasonably relied on Defendants to protect and safeguard their Private Information and to promptly and adequately inform them of the unauthorized Disclosure.

346. Defendants owed Plaintiffs and the Class a duty to maintain the privacy and security of Plaintiffs' and the Class's Private Information; take proper action to prevent the Disclosure; take proper action following the Disclosure to protect further unauthorized disclosure, release, and theft of Private Information, and promptly inform Plaintiffs and members of the Class about the breach.

347. Plaintiffs and members of the Class suffered ascertainable losses of money or property as a result of Defendants' use and employment of methods, acts, or practices declared to be unlawful by 73 Pa. Stat. §§ 201-2(2) and 201-(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs TACEY HABERKORN and JANE DOE, individually, and on behalf of all others similarly situated, pray for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and Plaintiffs' counsel as Class Counsel;

B. for an award of actual damages, compensatory damages, and statutory damages and penalties, in an amount to be determined, as allowable by law;

C. for an award of punitive damages, as allowable by law;

D. for equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

E. for equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

F. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

G. an order Defendants to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

H. for an award of attorneys' fees under the WESCA, the ECPA, the UTPCPL, the common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiffs

in connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

L.

JURY DEMAND

Plaintiffs, by counsel, hereby demand a trial by jury on all issues so triable.

Dated: November 27, 2023

Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops (*Pro Hac Vice*)
Amina A. Thomas (*Pro Hac Vice*)
Mary Kate Dugan (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice*)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice*)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Gary M. Klinger (*Pro Hac Vice* forthcoming)

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 West Monroe Street, Suite 2100
Chicago, Illinois 60606
(866) 252-0878
gklinger@milberg.com

Glen L. Abramson (PA Id. No. 78522)
Alexandra M. Honeycutt (*Pro Hac Vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 South Gay Street, Suite 1100
Knoxville, Tennessee 37929
(202) 932-7003
gabramson@milberg.com
ahoneycutt@milberg.com

Counsel for Plaintiffs and the Proposed Class